The National Science Foundation
Office of Polar Programs
United States Antarctic Program

Information Resource Management Directive 5000.11
USAP Information Resources Physical Security Policy

Organizational Function	Information Resource Management	Policy Number	5000.11
		Issue Date	1 August 2004
Policy Category	Information Security Policies and Procedures	Effective Date	1 August 2004
		Review On	1 August 2006
Subject	Information Resources Physical Security Policy	Authorized By	Director, OPP
Office of Primary Responsibility	National Science Foundation Office of Polar Programs Polar Research Support Section	Responsible Official	Mr. Patrick D. Smith Technology Development Manager
Address	Suite 755 4201 Wilson Blvd Arlington, VA 22230	Phone Fax Web	703.292.8032 703.292.9080 www.nsf.gov/od/opp
Distribution	USAP-Wide	Status	Final Policy
Online Publication	www.polar.org/infosec/index.htm		

1. PURPOSE

This directive establishes the requirements for physical security of information resources supporting the National Science Foundation (NSF) Office of Polar Programs (OPP), United States Antarctic Program (USAP). It identifies the physical security controls needed to protect information systems, facilities and supporting infrastructure from unauthorized access, natural disasters, or other threats.

2. BACKGROUND

Federal information technology regulations presented in OMB Circular A-130 and supporting legislation require the USAP to ensure all its information resources are physically secure against natural disaster, unauthorized access, or other threats.

3. GUIDING PRINCIPLES

- Physical security measures will be compatible with the life safety measures and logistical constraints unique to the Antarctic operating locations.
- Physical security measures will balance security needs with science and operations needs to support mission activities.

4. POLICY

All USAP information resources, facilities, and infrastructure elements will implement the appropriate level of physical security needed to protect the resources while supporting mission activities. This policy applies to all USAP information resources, and to all USAP operating locations.

4.1 Operational Definitions

4.1.1 Physical Security.

Physical security measures are steps taken to manage physical access to an information resource. Physical security is typically the first line of defense against theft, sabotage, and natural disasters. Examples of such measures are restrictions on entry to premises or equipment areas; locking, disabling, or disconnecting equipment; or the use of fire and tamper-resistant storage.

4.1.2 Environmental Controls.

Environmental control measures are steps taken to prevent or lessen damage to resources, or facilities due to changes in the system environment, or utility failures. Some examples are smoke detectors, uninterruptible power sources, fire suppression systems, and rerouting of plumbing systems.

4.1.3 Physical Access Controls.

Tangible means to prevent unauthorized physical access to an information resource. Examples are security guards, fences, locks, safes, sensors, or alarms.

4.1.4 Entry Controls.

Entry controls are the processes, procedures and supporting systems that manage physical access to information resources.

4.1.5 Physical Security Zoning.

The categorization of physical areas into zones, for the purpose of controlling access to information resources. The following zones are defined:

> **Zone 1: Public Access Permitted** - Areas open to the USAP general participant community.
>
> **Zone 2: Restricted Access** - Areas where unescorted access is restricted to the staff assigned to that area, and others with a management-approved need to access the area. Visitors may enter the area for a specific purpose, with an escort authorized to access the area.
>
> **Zone 3: Protected Access** - Access is controlled through proper identification. Visitors require management approval and must be escorted at all times.

4.1.6 Data Facilities.

A data facility is a room, closet, or other designated area used to support the USAP information infrastructure. Examples are server rooms, network operations centers, or distribution closets. In some instances, data facilities may be collocated with other utility

services, such as electrical closets. The term equipment room may also be used to describe a data facility.

4.1.7 Server Room.

A server room is a dedicated room for housing enterprise computing equipment, mainly servers, to better protect them against exposure to potential threats such as water, fire, smoke, heat, humidity or unauthorized human access. The terms Server Room, Data Center, and Computer Room may be used interchangeably.

4.1.8 Access Cards.

A physical control that uses a card, sometimes in conjunction with an access code or combination, to manage access to an area.

4.2 Access to Work Areas.

Access to work areas with information resources is normally restricted to USAP participants working or conducting business in that area.

4.3 After-hours Access.

All work areas with infrastructure connections will be secured after normal business hours, according to station operational requirements.

4.4 Sensitive Information Facilities & Resources.

Physical access to USAP information facilities and resources used for sensitive information, or for providing infrastructure support, will be controlled using appropriate measures such as guards, identification badges, locks, or access cards.

4.5 Unoccupied Work Areas.

When a work area will be unoccupied because the occupant is away on business, personal leave, deployment, or has left the program, their work area infrastructure connections will be disabled until their return.

4.6 Data Facility Conditions.

All USAP data facilities will have protective measures against water, fire, dust, dirt, smoke, extreme temperature, humidity, as well as a controlled access for authorized personnel. All areas will be kept free of debris, clutter, and non-essential equipment items. Data facilities will not be used for storage of equipment, materials, tools or supplies, unless the facility has been designed to accommodate such items.

4.7 Physical Inventory.

The USAP Prime Contractor will establish and maintain an inventory of all USAP information resources, noting in particular the equipment serial number and date the equipment entered service. The inventory will be physically audited and updated annually.

4.8 Reporting Unauthorized Access.

All USAP participants will report any unauthorized access, entry, or suspicious activity to their supervisors or to security personnel immediately upon detection.

4.9 Zoning of Work Areas.

The USAP Information Security Manager and the USAP participant organizations will recommend specific zoning for USAP work areas according to the work performed, and the degree to which sensitive information is processed within the work area.

4.10 Storage Media Controls.

The USAP participant organizations will maintain logs of who deposits and withdraws tape backups and other storage media from libraries.

4.11 Management of Physical Access.

The USAP participant organizations will ensure access codes, combinations, and other entry controls are changed on a periodic basis, or after personnel transitions, or an unauthorized access. At a minimum, access codes, combinations, or other entry controls will be changed every 90 days. The USAP Information Security Manager will identify procedures

4.12 Visitors & Temporary Personnel.

The USAP shall insure all visitors, contractors, and maintenance personnel requiring temporary access to sensitive areas are properly authenticated through the use of preplanned appointments, identification checks, appropriate escort, and sign-in and sign-out logs. Visitors and temporary workers must be announced, sponsored by an authorized USAP participant, and escorted in areas requiring escorted access.

4.13 Computer Monitor Position.

In work areas where sensitive information is processed, computer monitors will be positioned to eliminate viewing by unauthorized persons. In areas where physical changes to the position of the monitor may not be possible, the information resource user will implement other methods to ensure sensitive information is properly protected.

5. APPLICABILITY AND COMPLIANCE

This policy applies to all information resources, systems, and technology and to all users of these resources, systems and technology within the USAP operating environment or connected to the USAP information infrastructure. Compliance with this policy is as indicated in USAP Information Security Policy 5000.1, *The USAP Information Security Program*

6. RESPONSIBILITIES

Within the NSF and the USAP, several elements have specific responsibilities that directly affect the security of information resources and information systems.

6.1 USAP Information Security Manager.

The USAP Information Security Manager (ISM) develops and implements processes, standards, and procedures for physical security of USAP information resources.

6.2 USAP Information Systems Managers and Administrators.

The systems managers and administrators for USAP information systems ensure their systems implement proper physical security measures commensurate with the risks identified for their systems..

7. INFORMATION RESOURCES PHYSICAL SECURITY IMPLEMENTATION

7.1 Implementation

The NSF OPP and USAP participant organizations responsible for station operations will identify special circumstances which could affect their ability to completely implement this policy, and coordinate waivers with the OPP Technology Manager and the USAP Information Security Manager.

7.2 Policy Review.

The USAP Information Security Manager will review this policy in conjunction with major changes to the information infrastructure, as part of the USAP's participation in agency security audits, after each breach in system security, or every two years. The ISM will submit policy changes and new policies for review and approval by NSF OPP.

8. AUTHORITY

Publication of this policy is in conformance with the authority of the National Science Foundation Act of 1950, as amended and extended, the Federal Information Security Management Act of 2002 and NSF Manual 7, The NSF Information Security Handbook.

KARL A. ERB
Director